

# Docker Firewall Configuration

Source: [Firewalld Strict Docker Filtering](#)

## Preparation

Required parts:

Install firewalld and activate service:

```
pacman -Syu firewalld
systemctl enable --now firewalld.service
```

Disable any other firewall services.

Disable iptables for docker by adding or changing `/etc/docker/daemon.json` by adding the following config options:

```
{
  "iptables": false
}
```

After changing this config file, restart the Docker daemon to apply the previous change:

```
systemctl restart docker.service
```

As a result of the previous steps, only allowed ports on firewalld are accessible from the outside. However containers are now unable to connect outbound to the internet.

## firewalld Configuration

### Allow internet access for Docker containers

We need to allow masquerading to allow traffic from the Docker zone to the internet:

```
# Running this command allows your containers to reach out to the internet
firewall-cmd --permanent --zone=home --add-masquerade
# Since we used the --permanent flag, we need to reload the firewall for the changes to take
effect
firewall-cmd --reload
```

Docker creates a zone in firewalld specifically for its bridge network interfaces for each container network along with the docker0 interface.

To fix networking for containers that are not connected to a docker network, add your network interface connected to the network to the masqueraded zone.

---

Revision #7

Created 16 May 2023 00:02:46

Updated 14 September 2024 03:22:26 by etorres